UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/681,279	03/13/2001	Roy Myron Pueschel		7869

27943 7590 09/01/2004

ROY M. PUESCHEL
80 DRINKWATER RD.
HAMPTON FALLS, NH 03844

EXAMINER	
SIMITOSKI, MICHAEL J	

ART UNIT	PAPER NUMBER
2134	

DATE MAILED: 09/01/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/681,279	PUESCHEL, ROY MYRON	
	Examiner	Art Unit	
	Michael J Simitoski	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *13 March 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-22* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-22* is/are rejected.

7)☒ Claim(s) *1-22* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *13 March 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-22 are pending.

2. The petition of 4/13/01 has been granted.

Specification

3. The specification is objected to as failing to provide proper antecedent basis for the claimed subject matter. See 37 CFR 1.75(d)(1) and MPEP § 608.01(o). Correction of the following is required:

The "generated random number" of claim 8 is not disclosed in the specification,

The "preset channels" of claim 8 are not disclosed in the specification.

The "regenerating the node" in claim 18 is not disclosed in the specification.

Claim Objections

4. Claims 1-22 are objected to because of the following informalities:

Regarding claim 1, the preamble should begin similarly to the following example: "A method of regulating the use of encrypted freely distributed files and streams by a user comprising the steps of: ...",

Regarding claim 1, the phrase "loading self-installing" should be replaced with "loading a self-installing".

Regarding claim 1, the phrase "on user's target computer" should be replaced with "on a user's target computer".

Regarding claim 6, the phrase "the particular file" should be replaced with "a particular file" to avoid lack of antecedent basis in the claim.

Regarding claim 12, "by network connection" should be replaced with "by a network connection" or equivalent such as "via network connection".

Regarding claim 15, "by network connection" should be replaced with "by a network connection" or equivalent such as "via network connection".

Regarding claim 19, "digital equipment; the node is of such" should be replaced with "digital equipment, the node being of such".

Regarding claim 18, "network connection" should be replaced with "a network connection" to avoid a lack of antecedent basis.

Regarding claim 21, the claim is in improper form because the claim depends on both claim 1 and claim 7, rendering the scope indefinite. Accordingly, the claim has not been further treated on the merits.

Appropriate correction is required.

Claim Rejections - 35 USC § 112

5. The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

6. Claim 1-22 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement. The claim(s) contains subject matter which was not described in

the specification in such a way as to enable one skilled in the art to which it pertains, or with which it is most nearly connected, to make and/or use the invention.

Regarding claim 1, the concept of a "complex" node is, while mentioned, not described in the specification; the scope of the term "complex node" is therefore not enabled. *For the purposes of this Office Action, "complex node" will be understood to refer to the software node of the specification that uses policy and credit objects to use encrypted files and streams on behalf of a local computer.*

Regarding claim 1, the limitation that the node is "self-installing" is not described in the specification. *For the purposes of this Office Action, "self-installing" is understood to mean that once initiated, a node will execute an installation routine to install the node (such as is done in a standard software installation).*

Regarding claim 7, the limitation "other exchange locations" is not described in any detail in the specification in such a way as to enable the limitation.

Regarding claim 8, the limitation "channel sequences" is not described in the specification in such a way as to enable the limitation.

Regarding claim 9, the limitation "calibration of time" is not described in the specification in such a way as to enable the limitation.

Regarding claim 12, the limitation "security object source" is not enabled in the specification. *For the purposes of this Office Action, "security object source" is understood to mean "controlling authority" as is described in the specification as the source for secret keys, policy objects and credit objects.*

Regarding claim 17, the limitation "complex memory locations" is not enabled in the specification. *For the purposes of this Office Action, "complex memory locations" is understood to mean the memory used by an operating system.*

Regarding claim 18, the limitation "regenerating the node in claim 4 locally" is not enabled in the specification. *For the purposes of this Office Action, "regenerating the node" is understood to mean "updating the node".*

7. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

8. Claims 1-22 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Regarding claim 1, the limitation "self-installing" is unclear, as the computer literature generally associates an installation with the "loading" process (from a disk/media), which according to the claim is executed by some external means; it is unclear what defines a node/software as "self-installing".

Regarding claim 2, the claim depends from a method of "regulating the use ..." and therefore is unclear. *For the purposes of this Office Action, the claim is understood to read* "The method of claim 1, wherein the node is loaded from data media such as a floppy diskette or CD."

Regarding claim 2, the phrase "such as" renders the claim indefinite because it is unclear whether the limitations following the phrase are part of the claimed invention. See MPEP § 2173.05(d).

Regarding claim 3, the claim depends from a method of "regulating the use ..." and therefore is unclear. *For the purposes of this Office Action, the claim is understood to read* "The method of claim 1, wherein the node is loaded from a network connection."

Regarding claim 4, the claim depends from a method of "regulating the use ..." and therefore is unclear. *For the purposes of this Office Action, the claim is understood to read* "The method of claim 1, further comprising the steps of requiring said self-installing node to obtain a network connection ...".

Regarding claim 4, the limitation "in a unique and complex fashion" is vague and indefinite. *The term "complex" will be understood to mean difficult to defeat.*

Regarding claim 5, the claim depends from claim 4 and therefore the preamble renders the claim unclear. *For the purposes of this Office Action, the claim is understood to read* "The method of claim 4, wherein the installation of said node upon said target computer is performed in a fashion providing sufficient complexity and variety so as to make the unauthorized ...".

Regarding claim 5, the limitation "sufficient complexity and variety" is vague and indefinite. *The term "complex" will be understood to mean difficult to defeat.*

Regarding claim 5, the limitation "practically impossible" is vague and indefinite.

Regarding claim 6, the claim depends from claim 1 and therefore, the preamble renders the claim unclear. *For the purposes of this Office Action, the claim is understood to read* "The method of claim 1, further comprising the steps of the node partially decrypting said encrypted files and streams using the secret key associated with the particular file or stream."

Regarding claim 6, the claim recites the limitation "the secret key" in line 2. There is insufficient antecedent basis for this limitation in the claim.

Regarding claim 6, the claim recites the limitation "the particular file or stream" in line 2. There is insufficient antecedent basis for this limitation in the claim.

Regarding claim 7, the claim depends from claim 1 and therefore, the preamble renders the claim unclear. *For the purposes of this Office Action, the claim is understood to read* "The method of claim 1, further comprising the step of sending partially decrypted data between said node and the application that uses the decrypted file or stream through channels, which are one or more memory and other exchange locations in the target computer.".

Regarding claim 7, the claim recites the limitation "the application" in line 2. There is insufficient antecedent basis for this limitation in the claim.

Regarding claim 7, the claim recites the limitation "the decrypted file or stream" in line 2. There is insufficient antecedent basis for this limitation in the claim.

Regarding claim 8, the claim depends from claim 7 and therefore, the preamble renders the claim unclear. *For the purposes of this Office Action, the claim is understood to read* "The method of claim 7, wherein the data is partially decrypted using associated keys and channels, such that said channel communications are initiated with preset channels between said node and said application, and a generated random number is passed over said channels, and used thereafter to determine channel sequences throughout data transmission from the node to the application."

Regarding claim 9, the claim depends from claim 1 and therefore, the preamble renders the claim unclear. *For the purposes of this Office Action, the claim is understood to read* "The method of claim 1, further comprising the step of updating said node at intervals of time via network connection to provide improvement of security by changing node characteristics such as

any of the following: said node secret key, encryption algorithm, channel patterns, unique identification, or calibration of time."

Regarding claim 9, the phrase "such as" renders the claim indefinite because it is unclear whether the limitations following the phrase are part of the claimed invention. See MPEP § 2173.05(d).

Regarding claim 9, the claim recites the limitation "said node secret key, encryption algorithm, channel patterns, unique identification, or calibration of time" in lines 3-4. There is insufficient antecedent basis for this limitation in the claim.

Regarding claim 10, the claim depends from claim 9 and therefore, the preamble renders the claim unclear. *For the purposes of this Office Action, the claim is understood to read* "The method of claim 9, wherein the steps of sending and receiving are performed for any data exchange which requires security on the local computer."

Regarding claim 11, it is unclear what limitations are presented in the claim. *For the purposes of this Office Action, the claim is understood to read* "The method of claim 1, further comprising the step of determining policy from said encrypted policy objects and their respective public keys."

Regarding claim 11, the claim recites the limitation "their respective public keys" in lines 1-2. There is insufficient antecedent basis for this limitation in the claim.

Regarding claim 12, the claim depends from claim 11 and therefore, the preamble renders the claim unclear. *For the purposes of this Office Action, the claim is understood to read* "The method of claim 11, further comprising the steps of receiving and loading said encrypted policy

objects and said public keys onto said user's target computer by network connection from a security object source."

Regarding claim 13, the claim depends from claim 12 and therefore, the preamble renders the claim unclear. *For the purposes of this Office Action, the claim is understood to read* "The method of claim 12, further comprising the step of updating said policy object at intervals of time via network connection to keep loaded policy objects current."

Regarding claim 14, the claim depends from claim 1 and therefore, the preamble renders the claim unclear. *For the purposes of this Office Action, the claim is understood to read* "The method of claim 1, further comprising the step of determining credit from said encrypted credit objects and said encrypted secret keys."

Regarding claim 14, the claim recites the limitation "said encrypted secret keys" in lines 1-2. There is insufficient antecedent basis for this limitation in the claim.

Regarding claim 15, the claim depends from claim 14 and therefore, the preamble renders the claim unclear. *For the purposes of this Office Action, the claim is understood to read* "The method of claim 14, further comprising the step of receiving and loading said encrypted credit objects and said encrypted secret keys onto said user's target computer by network connection from a security object source."

Regarding claim 16, the claim depends from claim 15 and therefore, the preamble renders the claim unclear. *For the purposes of this Office Action, the claim is understood to read* "The method of claim 15, further comprising the step of decrypting said encrypted secret keys with the target node's secret key."

Regarding claim 17, the claim appears to depend on itself. *For the purposes of this Office Action, claim 17 is understood to depend from claim 7.*

Regarding claim 17, as best understood, the claim depends from claim 7 and therefore, the preamble renders the claim unclear. *For the purposes of this Office Action, the claim is understood to read* "The method of claim 7, further comprising the step of securely storing said encrypted objects and said decrypted secret keys as distributed throughout the target the target node's complex memory locations."

Regarding claim 17, the term "complex" in claim 17 is a relative term which renders the claim indefinite. The term "complex" is not defined by the claim, the specification does not provide a standard for ascertaining the requisite degree, and one of ordinary skill in the art would not be reasonably apprised of the scope of the invention. *The term "complex" will be understood to mean difficult to defeat.*

Regarding claim 17, the claim recites the limitation "the target node's complex memory locations" in lines 2-3. There is insufficient antecedent basis for this limitation in the claim.

Regarding claim 18, the claim depends from claim 4 and therefore, the preamble renders the claim unclear. *For the purposes of this Office Action, the claim is understood to read* "The method of claim 4, further comprising the step of regenerating the node locally through network connection to the node originator. Node modifications are transmitted over the network and stored on the local computer."

Regarding claim 18, the claim recites the limitation "the local computer" in line 3. There is insufficient antecedent basis for this limitation in the claim.

Regarding claim 19, the claim depends from claim 1 and therefore, the preamble renders the claim unclear. *For the purposes of this Office Action, the claim is understood to read* "The method of claim 1, further comprising the steps of: creating a unique node installation for a computer or digital equipment, the node is of such complexity and uniqueness as to require an installation program, generating a unique installation program to install said unique node."

Regarding claim 19, "the node is of such complexity and uniqueness" is vague and indefinite. *The term "complex" will be understood to mean difficult to defeat.*

Regarding claim 19, the claim recites the limitation "said unique node" in line 6. There is insufficient antecedent basis for this limitation in the claim.

Regarding claim 20, the claim depends from claim 1 and therefore, the preamble renders the claim unclear. *For the purposes of this Office Action, the claim is understood to read* "The method of claim 1, further comprising the steps of generating the encrypted files and streams, by a file or streams source, and their identification headers that are associated with encrypted policy objects. Encryption of files and streams may be partial, intermittent or complete; generating the secret public keys used to decrypt the files and streams."

Regarding claim 20, the claim recites the limitation "the secret public keys" in line 6. There is insufficient antecedent basis for this limitation in the claim.

Regarding claim 20, it is unclear whether "secret public keys" refers to secret keys or public keys. *For the purposes of this Office Action, "secret public keys" is assumed to mean secret keys.*

Regarding claim 22, the claim depends from claim 1 and therefore, the preamble renders the claim unclear. *For the purposes of this Office Action, the claim is understood to read* "The

method of claim 1, further comprising the steps of: generating the public keys used to decrypt the policy objects; generating encrypted policy objects with public keys. The policy objects are associated with a file or stream; generating encrypted credit objects with or without encrypted secret keys that are associated with either individual or groups of files or streams."

Regarding claim 22, the claim recites the limitation "the public keys" in line 3. There is insufficient antecedent basis for this limitation in the claim.

Regarding claim 22, it is unclear whether the limitation "that are associated" is referring to "encrypted credit objects" or the "encrypted secret keys". *For the purposes of this Office Action, the encrypted secret keys are understood to be associated with the files or stream.*

Regarding claim 22, "generating encrypted policy objects with public keys" implies that the policy objects are encrypted with public keys, however, the limitation "generating the public keys used to decrypt the policy objects" the this, because it is well established in the art of public key cryptography that a piece of data encrypted with a public key is only decrypted with the private key associated with the public key. *For the purposes of this Office Action, the second limitation in the claim will be read as "generating encrypted policy objects with secret keys ...".*

9. Claims 18, 20 & 22 are rejected as failing to define the invention in the manner required by 35 U.S.C. 112, second paragraph.

The claim(s) must be in one sentence form only. Note the format of the claims in the patent(s) cited.

10. The above claim suggests are not meant to indicate allowable claims or subject matter, but merely to suggest a general structure for standard preambles form. See the attached patent references for further examples. When drafting any amendments to the claims, all stated

rejections and objections in this Office Action should be considered. Applicant should be careful not to introduce any new matter into the disclosure (i.e., matter which is not supported by the disclosure as originally filed).

Claim Rejections - 35 USC § 103

11. To expedite a complete examination of the instant application, the claims rejected under 35 U.S.C. 112 are further rejected as set forth below as best understood.

12. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

13. Claims 1-7, 14, 17 & 19-20 are rejected under 35 U.S.C. 103(a) as being unpatentable over "DigiBox: A Self-Protecting Container for Information Commerce" by Sibert et al. (Sibert) in view of U.S. Patent 5,915,019 to Ginter et al. (Ginter).

Regarding claims 1, 4 & 5, Sibert discloses loading a self-installing complex node/software implementation on a user's target computer (§5.4 ¶2-3), installing said complex node on said user's target computer (§5.4 ¶2-3) and using said encrypted files and streams (§4.1 & §5.3) through secure local decryption (§3.3, §5.3 & Figs. 5-6) by means of said installed node/software implementation (§5.4) and by means of encrypted policy objects/control sets (§4.2, §5.1 ¶2 & Fig. 4). Sibert lacks credit objects. However, Ginter teaches that credit objects/traveling objects are used to enable at least one or more types of object content. The traveling objects can be stored and managed on the local VDE node (col. 130, line 38 – col. 131,

line 29 & col. 127, line 57 – col. 129, line 22). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to use encrypted credit objects. One of ordinary skill in the art would have been motivated to perform such a modification to enable budgeting and content usage, as taught by Ginter (col. 130, line 38 – col. 131, line 29 & col. 127, line 57 – col. 129, line 22).

Regarding claims 2 & 3, Sibert, as modified above, lacks installing the node/software implementation from a data media or a network connection. However, the examiner takes Official Notice that installing software via data media and network installation is old and well established in the art of software management as a method of distributing and installing applications. Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to load the node on a user's target computer from a data media or network connection. One of ordinary skill in the art would have been motivated to perform such a modification to utilize well-known methods of software installation. This advantage is well known to those skilled in the art.

Regarding claim 6, Sibert discloses the DigiBox creator partially encrypting files and streams using a secret key associated with the particular file or stream (§5.2 ¶2-3 & §5.3 ¶3-4). While Sibert does not disclose the node decrypting the data, it is inherent that it is done, in light of §4 ¶5, §5.1 ¶4 & §5.2 ¶3-4, the purpose of the DigiBox system being the delivery and use of protected data.

Regarding claims 7 & 17, Sibert, as modified above, lacks sending data between applications through channels, which are one or more memory and other exchange locations in the target computer. However, Ginter teaches that channels are used in a DMA controller to

handle multiple transfers simultaneously from a microprocessor and between components of the SPU (RAM, ROM) (col. 68, lines 50-64). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to send data between the node and application using the file by way of channels. One of ordinary skill in the art would have been motivated to perform such a modification to enable multiple transfers to occur simultaneously, as taught by Ginter (col. 68, lines 50-64).

Regarding claim 14, Sibert, as modified above, discloses determining credit from the encrypted credit objects and encrypted secret keys (Ginter, col. 132, lines 18-28). Further, the examiner takes Official Notice that installing software via network installation is old and well established in the art of software management as a method of distributing and installing applications. Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to load the node on a user's target computer from a network connection. One of ordinary skill in the art would have been motivated to perform such a modification to utilize well-known methods of software installation. This advantage is well known to those skilled in the art.

Regarding claim 19, Sibert, as modified above, lacks creating a unique installation and installation program for a node. However, Sibert teaches that one known method of software distribution is the "cryptographic lock" wherein the software installation is unique in that it requires a unit code to enable it (§3.3). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to generate a unique installation and installation program. One of ordinary skill in the art would have been motivated to perform such

a modification to take advantage of a known mechanism in distributing software, as taught by Sibert (§3.3).

Regarding claim 20, Sibert discloses generating encrypted files or streams (§5.2 ¶2-3) by a source (DigiBox packaging application) (Fig. 3) and their identification headers (§5.2 ¶1) that are associated with encrypted policy objects/control sets (§4.2). While Sibert lacks explicit disclosure of generating the secret keys to decrypt the streams, it is inherent that this must be done before the user can use the encrypted data.

14. Claim 8 is rejected under 35 U.S.C. 103(a) as being unpatentable over Sibert in view of Ginter, as applied to claim 1 above, in further view of U.S. Patent 5,386,532 to Sodos. Sibert, as modified above, lacks a generated random number used to determine channel sequences. However, Sodos teaches that random DMA channel sequences (col. 6, lines 1-4) are used to allow for multiple interleaving DMA channels (col. 3, lines 1-25). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to generate a random number to determined channel sequences. One of ordinary skill in the art would have been motivated to perform such a modification to allow for multiple interleaving DMA channels, as taught by Sodos (col. 3, lines 1-25 & col. 6, lines 1-4). While Sodos lacks explicit disclosure of initiating with preset channels, it is inherently done so the channel sequence can be established.

15. Claims 9-13, 15, 16 & 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Sibert in view of Ginter, as applied to claim 1 above, in further view of Applied Cryptography, Second Edition by Schneier.

Regarding claims 9-10, Sibert, as modified above, lacks periodically updating the node characteristics. However, Schneier teaches that no key should ever be used for an indefinite period of time (§8.10) and should be replaced regularly (§8.11). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to update the node secret key at intervals/regularly. One of ordinary skill in the art would have been motivated to perform such a modification to alleviate the security risks associated with stale keys, as taught by Schneier (§8.10-8.11).

Regarding claim 11, Sibert, as modified above, discloses encrypted policy objects being encrypted and verified with a hash function, but lacks specifically using public keys. However, Schneier teaches the well-known concept of digital signatures, where a document is signed with a private key of the owner and a verifier uses the public key to verify that the data hasn't been modified (page 37). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to determine policy objects from said encrypted policy objects and their respective public keys. One of ordinary skill in the art would have been motivated to perform such a modification to verify that the data hasn't been modified, as taught by Schneier (page 37).

Regarding claims 12 & 15, Sibert, as modified above, discloses loading encrypted policy objects/control sets security object source (DigiBox packaging application) (Fig. 3), but lacks loading public keys from the source. However, because the DigiBox packaging application will

necessarily know the private key used to encrypt the package, as modified above by Schneier (page 37), it would have to have and disclose the public key. Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to load the public keys to the target computer from the DigiBox packaging application. One of ordinary skill in the art would have been motivated to perform such a modification because the DigiBox application necessarily knows the private key used to encrypt and sign the package, as taught by Schneier (page 37) and must deliver the public key as per the public/private key concept. Further, the examiner takes Official Notice that installing software via network installation is old and well established in the art of software management as a method of distributing and installing applications. Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to load the node on a user's target computer from a network connection. One of ordinary skill in the art would have been motivated to perform such a modification to utilize well-known methods of software installation. This advantage is well known to those skilled in the art.

Regarding claim 13, Sibert, as modified above, lacks periodically updating the node policy object. However, Schneier teaches that no key should ever be used for an indefinite period of time (§8.10) and should be replaced regularly (§8.11). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to update the node key and hence the encrypted policy objects at intervals/regularly. One of ordinary skill in the art would have been motivated to perform such a modification to alleviate the security risks associated with stale keys, as taught by Schneier (§8.10-8.11).

Regarding claim 16, Sibert, as modified above, lacks decrypting the encrypted secret keys with the target node's secret key. However, Schneier teaches that using public-key cryptography to exchange keys makes key-exchange easier (page 48). The key/secret key is exchanged by decrypting it with the receiver's private key (page 48). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to decrypt the encrypted secret keys with the target node's secret key. One of ordinary skill in the art would have been motivated to perform such a modification to make key-exchange easier by using public-key cryptography, as taught by Schneier (page 48).

Regarding claim 22, Sibert, as modified above, lacks explicit disclosure of generating the public keys, generating encrypted policy objects/control sets and generating encrypted credit objects. However, as modified by Ginter to include credit objects, and by Schneier to include public keys above, it is inherent that the encrypted policy objects, credit objects and secret keys are generated, as they are used.

Conclusion

16. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael J. Simitoski whose telephone number is (703)305-8191. The examiner can normally be reached on Monday - Thursday, 6:45 a.m. - 4:15 p.m.. The examiner can also be reached on alternate Fridays from 6:45 a.m. – 3:15 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse can be reached on (703)308-4789.

Any response to this action should be mailed to:
Commissioner of Patents and Trademarks

Washington, DC 20231

Or faxed to:

(703)746-7239 (for formal communications intended for entry)

Or:

(703)746-7240 (for informal or draft communications, please label "PROPOSED" or "DRAFT")

Hand-delivered responses should be brought to Crystal Park II, 2121 Crystal Drive, Arlington, VA 22202, Fourth Floor (Receptionist).

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-9000.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

MJS
August 23, 2004

GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100